



TRABAJO DE FIN DE GRADO

GRADO EN DERECHO FACULTAD DE DERECHO

CURSO ACADÉMICO 2019-2020

PROTECCIÓN DE DATOS DATA PROTECTION

AUTOR: MAURO CARRANCIO CALVO

DIRECTOR/A: VICTORIA ORTEGA BENITO

**1. INTRODUCCIÓN Y QUE ES Y COMO SE DESARROLLA
LA PROTECCIÓN DE DATOS..... 4 - 8**

**2. NORMATIVA EUROPEA DE PROTECCIÓN DE DATOS..
8- 16**

**2.1. NORMAS PRECEDENTES AL REGLAMENTO GENERAL
DE PROTECCIÓN DE DATOS..... 9 - 15**

2.1.1. Convenio 108 del Consejo de Europa 9 - 12

2.2.2. Directiva 95/46/CE 12 - 15

**2.2. NORMAS ACTUALES EN MATERIA DE PROTECCIÓN DE
DATOS..... 15 - 16**

**2.2.1. Reglamento (UE) 2016/679 del Parlamento Europeo y
del Consejo del 27 de Abril de 2016 (Reglamento general de
protección de datos)..... 15 - 16**

**3. NORMAS NACIONALES EN MATERIA DE PROTECCIÓN
DE DATOS..... 17 - 19**

**4. ÓRGANOS EUROPEOS EN MATERIA DE PROTECCIÓN
DE DATOS..... 19 - 23**

**4.1 SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS... 19
- 20**

4.2 COMITÉ EUROPEO DE PROTECCIÓN DE DATOS... 21 - 23

**5. ÓRGANOS ESTATALES DE PROTECCIÓN DE DATOS...
23 – 27**

**5.1 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS... 23 -
26**

5.2 DELEGADO DE PROTECCIÓN DE DATOS 26 - 27

**6. ÓRGANOS ESPECIALES EN CATALUÑA Y PAÍS VASCO
27 - 29**

**6.1 AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS...
28 - 29**

6.2 AGENCIA VASCA DE PROTECCIÓN DE DATOS.... 29

**7. ASPECTOS A DESTACAR DEL REGLAMENTO
GENERAL DE PROTECCIÓN DE DATOS... 30 - 33**

7.1 SANCIONES A EMPRESAS.... 30 - 31

7.2 CONSENTIMIENTO Y TRANSPARENCIA.... 31

7.3 REGISTRO DE ACTIVIDADES Y TRATAMIENTO.... 31

**7.4 ANÁLISIS DE RIESGOS Y EVALUACIONES DE
IMPACTO... 32**

7.5 EJERCICIO DE DERECHOS.... 32 - 33

7.6 TERCEROS... 33

7.7 BIG DATA 34

**8. CONCLUSIONES Y VISTAS AL FUTURO DE LA
PROTECCIÓN DE DATOS.... 34 – 36**

9. BIBLIOGRAFÍA... 37 – 40

1. INTRODUCCIÓN Y QUE ES Y COMO SE DESARROLLA LA PROTECCIÓN DE DATOS

Comenzamos con decir que en el mundo globalizado que nos encontramos ahora los datos van y vienen. Tenemos que tener en cuenta que ahora mismo las nuevas tecnologías nos proporcionan unas herramientas por las cuales cualquier persona puede compartir no solo sus datos sino también posar y adquirir los datos de otra persona de una manera bastante sencilla. Solo con el hecho de que los datos de una tercera persona hayan sido filtrados o esta persona los haya hecho públicos en la red podemos obtenerlos en pocos segundos. A raíz de esto se ha ido desarrollando una normativa tanto nacional, europea como internacional y que vamos a empezar a describir y acotar durante este trabajo.

Lo primero que cabe mencionar es el anclaje constitucional que tiene el derecho a la protección de datos para ello tenemos que referenciar el artículo 18.1 que nos esgrime lo siguiente “*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*”¹. Basándonos en esto el honor y la intimidad son dos conceptos que están relacionados con la protección de los datos personales.

Además esta protección de los datos personales quedaba ya refrendada por el Tribunal Constitucional en su sentencia 94/1998, de 4 de mayo, que nos alega: “*que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención*”².

Así mismo tenemos otra sentencia de referencia que es la Sentencia 292/2000 de 30 de noviembre que ya nos confirma que³ “*lo considera como un derecho autónomo e*

¹ Artículo 18.1 de la Constitución Española.

² Sentencia del Tribunal Constitucional 94/1998 de 4 de Mayo.

³ Sentencia del Tribunal Constitucional 292/2000 de 30 de Noviembre.

independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.”

Por lo tanto fijándonos en estas dos sentencias lo que se nos expone, es que este derecho se considera como un poder de decidir con quién o como compartes tus datos personales ya sea un tercero, el Estado o un particular. Además este derecho permite al individuo conocer quién posee los datos personales y en que sentido se están usando estos y con ello oponerse a ese uso y posesión.

Hay que considerar que la doctrina ha ido avanzando desarrollando este derecho más y más a lo largo del tiempo acomodándose a las necesidades que tenía debido a la injerencia de las nuevas tecnologías en este derecho. La doctrina relativa al derecho de la intimidad va evolucionando partiendo de un derecho pasivo de primera generación que proclamaba la “no injerencia en la vida privada” del individuo, llega a reivindicar un derecho de libertad informática o control de los datos personales incluidos en un fichero informático.⁴

Por lo tanto quiero remarcar que este derecho ha ido evolucionando durante los años y según lo que se esta viendo esta evolución no va a parar debido a que las nuevas tecnologías siguen avanzando e injeriendo en este derecho y para ello tendremos que crear normativa para parar y controlar esa ataque hacia el derecho a la intimidad.

Esta evolución de la que hablamos consta de tres generaciones. En efecto la doctrina distingue tres generaciones:

1. En la primera se configuran las libertades individuales frente a la injerencia de los poderes públicos, exigiendo sus límites y se tutelan por la observancia de derechos individuales.

⁴ Concepción Conde Ortiz. 2005. *La protección de datos personales un derecho autónomo con base en los conceptos de intimidad y privacidad*. Dykinson

2. En la segunda, desde el Estado Social de Derecho frente al Estado Liberal de Derecho, los derechos económicos, sociales y culturales exigen una política activa que garanticen su ejercicio.
3. En una tercera generación, se incluye la libertad informática como un nuevo derecho del individuo a tutelar su propia identidad informática, concretándose en las garantías de acceso y control de las informaciones procesadas en bancos de datos por parte de las personas a las que conciernen⁵

Nuestra normativa ha ido avanzando con estas generaciones. El desarrollo de este derecho fundamental de protección de los datos de las personas físicas tan importante en nuestro sistema jurídico tuvo su origen con la Ley Orgánica 5/1992, de 29 de Octubre, reguladora del tratamiento automatizado de datos cuya acrónimo era LORTAD.

Después de un tiempo, en concreto 7 años más tarde, fue sustituida por la Ley Orgánica del 15/1999, de 5 de diciembre, de protección de datos debido a que la Comunidad Europea (actual Unión Europea) dictó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, en relación con el tratamiento de datos personales y a la libre circulación de estos y España tenía la obligación de transponerla. Esta citada Directiva ya daba los primeros coletazos sobre como iba a desarrollar la protección de datos en el ámbito europeo y esto incluida a España.

La última generación se corresponde con la adopción del ya conocido por los expertos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016 o también llamado Reglamento general de protección de datos.

Aquí aparece la última actualización en el derecho español, esta es la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Esta ley aparece para regular distintos ámbitos que se pueden conjugar en 5 grupos:

⁵ SARDINA VENTOSA, F., op. cit., p.1

- I. Desarrollo del contenido del RGPD
- II. Regulación de determinados tratamientos específicos
- III. Nuevos derechos digitales
- IV. Régimen sancionador
- V. Estatuto y actuación de la AEPD ⁶

Estos cinco grupos son los más importantes y es lo que la ley se centra para desarrollar una protección especial en cuanto a este derecho fundamental que como ya hemos dicho se encuentra reflejado en el artículo 18.1 “ *Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*”⁷. Pero también en su apartado 4 que nos esgrime que “*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*”⁸

A raíz de esto la doctrina comenzó su estudio sobre lo que era la protección de los datos personales y podemos afirmar que el estudio de la llamada protección de datos personales se resume en tres características:

- a) Que los datos sean susceptibles de tratamiento o se encuentren en soporte susceptible de tratamiento
- b) Que se tenga la posibilidad de indentificar el resultado de los datos con su titular
- c) Que el manejo o acceso a los datos resulte sin consentimiento del titular ⁹

Para finalizar esta introducción hay que hacer hincapié de que este derecho colisiona con otros. Esto es un gran problema y como siempre se tiene que valorar que derecho prima sobre el otro en distintos casos. Actualmente hay un gran conflicto entre el derecho a la información y el derecho a la protección de esos datos personales.

⁶ Uría Menéndez. Diciembre 2018. *Principales novedades de la nueva Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales*. pág. 2.

⁷ Artículo 18.1 de la Constitución Española

⁸ Artículo 18.4 de la Constitución Española

⁹ Concepción Conde Ortiz. 2005. *La protección de datos personales un derecho autónomo con base en los conceptos de intimidad y privacidad*. Dykinson.

En la doctrina se afirma que el conflicto entre la libertad de información y de tratamiento de los datos -junto a la libertad de expresión-, y la intimidad, es uno de los grandes temas de nuestro tiempo que está generando múltiples estudios y provocando grandes y graves discrepancias doctrinales.¹⁰

Para la Ley de prensa, la intimidad era un límite al derecho a la información. El concepto de intimidad se refiere a lo interior, a lo más reservado, a lo más profundamente sentido por el ser humano. Se opone a lo público, a lo proclamado por todos.¹¹

Para terminar esta introducción, en la que he explicado que es y como se ha ido desarrollando a lo largo del tiempo hasta la actualidad la protección de datos personales. Cabe recordar que este derecho siempre va a colisionar con otros derechos y siempre va estar amenazado por las nuevas tecnologías.

También quería avanzar que en este trabajo vamos a tratar la normativa europea sobre la protección de datos y como no la normativa nacional que al final y al cabo se acopla a esa normativa superior de la Unión Europea. Además vamos referenciar y a explicar los distintos organismos públicos que existen para luchar por la protección de estos datos personales tanto en el ámbito nacional como internacional.

2. NORMATIVA EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS

En este epígrafe vamos a explicar cual es la normativa europea que es más importante y más destacable en materia de protección de datos. Además de hacer un recorrido sobre la como ha ido avanzado y desarrollandose el ordenamiento jurídico europeo en esta materia que estamos tratando. Desde las normas que preceden al gran y tan conocido Reglamento General de Protección de datos hasta llegar a este que también va ser explicado en profundidad.

¹⁰ DAVARA RODRÍGUEZ, M. A.: *La protección de datos personales en el sector de las telecomunicaciones*, cit., p. 9.

¹¹ URABAYEN, M., op. cit., p. 9

La normativa europea es la que crea el marco de referencia para que los 27 países europeos creen sus distintas leyes o normativas sobre la protección de datos.

Toda esta normativa pasa por un proceso de desarrollo de años yendo desde el Convenio 108 del Consejo de Europa pasando por la gran Directiva 95/46/CE hasta llegar como ya hemos dicho al Reglamento General de Protección de Datos.

En los siguientes puntos vamos a analizar los aspectos más importantes de estas leyes que crearon lo que hoy se entiende por protección de datos y que sin ellas este derecho no podría estar considerado como tal.

2.1 NORMAS PRECEDENTES AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS.

En este apartado vamos a identificar las dos grandes normas que son los precedentes del gran Reglamento General de Protección de datos que esta vigente ahora mismo.

Estas dos normas son el Convenio 108 del Consejo de Europa y la Directiva 95/46/CE. Ambas normas ya se encuentran derogadas debido a la introducción del Reglamento anteriormente mencionado. Pero estas normas sentaron los cimientos de lo que hoy es la protección de datos. En los siguientes epígrafes vamos a desarrollar estas normas profundamente.

2.1.1 Convenio nº 108 del Consejo de Europa

Para dar una introducción sobre instrumento lo primero que cabe decir es que este convenio fue aprobado el 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Tiene como fin garantizar a cualquier persona física «el respeto de

sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona»¹²

Hay que decir que España ratificó el Convenio del 31 de enero de 1984. También hay que remarcar que nuestro país ha venido incumpliendo algunas de las obligaciones jurídico-internacionales establecidas en su texto normativo, referidas precisamente a la elaboración y aprobación de una legislación interna¹³ y explicitadas en el art 4 del Convenio que nos dice lo siguiente *“1. Cada parte adoptará en su derecho interno las medidas necesarias para dar cumplimiento a los principios fundamentales de protección de datos enunciados en el presente capítulo. 2. Tales medidas deberán ser adoptadas como muy tarde en el momento en el que el presente Convenio entrare en vigor con respecto a la parte”* ¹⁴

Ahora bien después de explicar muy brevemente como España ratifico este convenio y como este país incumplio distintas obligaciones de transponer los distintos preceptos que tenía incorporados.

Este Convenio trata de armonizar «los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos» sobre la base de una serie de principios como la recogida lícita de datos, la calidad y confidencialidad de los datos sensibles, la información de la persona implicada y los derechos de acceso y de rectificación, ahora bien, siempre desde el convencimiento de que se trata de un Convenio de mínimos.¹⁵

Por lo tanto y como sabemos este es uno de los primeros instrumentos que regula y lleva a cabo una legislación de que como se debe articular la recogida lícita de datos, la

¹² La protección de datos personales (Enero de 2020). Recuperado de <https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales>

¹³ Cfr. S. Ripoll Carulla, “En torno a la calificación de la pasividad española en el cumplimiento del Convenio n.º 108 del Consejo de Europa como acto ilícito internacional”, en *La responsabilidad internacional*, XII Jornadas de la A.E.P.D.I.R.I., Alicante, 1990, págs. 313 - 330

¹⁴ Artículo 4 del Convenio 108 del Consejo de Europa

¹⁵ D. Juan Antonio Pavón Perez (Profesor de Derecho Internacional Público). Universidad de Extremadura. *La protección de datos personales en el consejo de europa: El protocolo adicional al Convenio 108 Relativo a las autoridades de control y a los flujos transfronterizos de datos personales.*

calidad y confidencialidad de los mismos. Es el primer Convenio que trata de legislar sobre esta materia tan complicada y trata de valorar entre la libre circulación de los datos entre distintas personas o sociedades y el traspaso o como lo llama específicamente el Convenio “recogida lícita de datos”.

Es por ello que el Convenio pretende compatibilizar en todo momento la protección del derecho a la intimidad personal ¹⁶ con la liberalización de los flujos de datos entre Estados partes, siendo así que la libre circulación de los datos de carácter personal entre los Estados signatarios solo decaerá en dos supuestos:

1. Cuando la protección de datos de carácter personal no sea equivalente en la otra parte.
2. Cuando la transmisión de los mismos se realice a un tercer Estado que no sea parte en el Convenio ¹⁷

Así mismo este Convenio no es parte en si de la Unión Europea si no que ha sido promulgado por el Consejo de Europa el 28 de enero de 1981.

Finalmente y para acabar este epígrafe quería decir que este Convenio no puede asumir toda la complejidad de la materia de la protección de datos y por ello el propio Consejo de Europa ha llegado a adoptar una serie de recomendaciones de carácter sectorial que se dirigen directamente al propio gobierno tanto sobre datos estadísticos¹⁸, datos médicos¹⁹.

¹⁶ Vid. J. Carrascosa González, «Protección de la intimidad y tratamiento automatizado de datos de carácter personal en Derecho internacional Privado», Revista Española de Derecho Internacional, vol. XLIV, 1992, págs. 417-441; G. Garzón y E. Vilariño, «Information and Privacy Protection in TDF: The Rights Involved», en O.C.D.E., TDF and the Protection of Privacy, págs. 306 y ss; D. H. Flaherty, Privacy and Government Data Banks: an International Perspective, Londres, Mansell, 1979; R. N. Savage y I. N. Waldenn, «Data Protection and Privacy Laws: Should Organisations Be Protected», I.C.L.Q., 1988, págs. 37 y ss.

¹⁷ D. Juan Antonio Pavón Perez (Profesor de Derecho Internacional Público). Universidad de Extremadura. *La protección de datos personales en el consejo de europa: El protocolo adicional al Convenio 108 Relativo a las autoridades de control y a los flujos transfronterizos de datos personales.*

¹⁸ Recomendación Núm. R (83) 10, relativa a la protección de datos personales utilizados en investigaciones científicas y estadísticas. Adoptada por el Comité de Ministros el 23 de septiembre de 1983; Recomendación Núm. R (97) 18 sobre la protección de datos personales recopilados y tratados con fines estadísticos. Adoptada por el Comité de Ministros el 30 de septiembre de 1997.

¹⁹ Recomendación Núm. R (81) 1, relativa a la reglamentación aplicable a los bancos de datos médicos automatizados. Adoptada por el Comité de Ministros el 23 de enero de 1981. Asimismo, la Recomendación Núm. R (97) 5, relativa a la protección de datos médicos. Adoptada por el Comité de Ministros el 13 de febrero de 1997. Sobre la protección de datos médicos y genéticos en el Consejo de Europa véanse, entre

2.1.2 Directiva 95/46/CE

Esta directiva se consideraba el texto de referencia en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE).²⁰ Por lo tanto podríamos llegar a decir que este es el gran origen del Reglamento General de Protección de datos que tanto hemos nombrado anteriormente.

Así mismo esta Directiva tiene como objeto crear unos límites para la recogida y utilización de datos personales. También esta directiva trata de armonizar la situación de protección de datos personales en cada Estado miembro creando una legislación europea para todos.

Sabemos que esta Directiva se aplica a los datos tanto informatizados como a los datos que se encuentren en ficheros de papel tradicionales. En este caso la Directiva no se aplicará al tratamiento de datos:

- efectuado por una persona física en el ejercicio de actividades exclusivamente particulares o domésticas;
- aplicado al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, tales como la seguridad pública, la defensa o la seguridad del Estado.²¹

otros, S. Ripio Carulla, «La protección de los datos médicos y genéticos en la normativa del Consejo de Europa (Parte I)», Revista de Derecho y Genoma Humano, n.º 5/1996, págs. 117-131; del mismo autor, «La protección de los datos médicos y genéticos en la normativa del Consejo de Europa (Parte II)», Revista de Derecho y Genoma Humano, n.º 6/1997, págs. 111-140; M. Serrano Pérez, «La protección de datos relativos a la salud en la legislación española y en la normativa comunitaria», Noticias de la Unión Europea, n.º 187-188, agosto/septiembre 2000, págs. 59-68.

²⁰ Protección de datos personales (8 de marzo de 2014) Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3A114012>

²¹ Protección de datos personales (8 de marzo de 2014) Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3A114012>

La propia Directiva tiene como objeto proteger todos los derechos y libertades de las personas en cuanto al tratamiento de datos personales. Es la propia Directiva la que nos ratifica cuando es lícito el tratamiento de datos.

El tratamiento de datos solo es lícito si:

- el interesado ha dado inequívocamente su consentimiento
- el tratamiento es necesario para el cumplimiento de un contrato en el que sea parte el interesado.
- el tratamiento es necesario para el cumplimiento de una obligación legal del responsable del tratamiento;
- el tratamiento es necesario para proteger los intereses vitales de la persona de cuyos datos se trate;
- el tratamiento es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero.
- el tratamiento es necesario para los fines de interés legítimo del responsable del tratamiento o de un tercero, siempre que sobre dichos intereses no prevalezcan los intereses del interesado en el ámbito de los derechos y libertades que requieren protección.²²

Es la propia Directiva la que nos referencia que derechos tienen los interesados cuando sus datos son tratados.

En primer lugar se entiende que existe un derecho a obtener información: el responsable del tratamiento deberá facilitar cierta cantidad de información (identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, etc.).

En segundo lugar, el derecho de acceso del interesado a los datos: El derecho de acceso del interesado a los datos: todos los interesados deberán tener el derecho de obtener del responsable del tratamiento.

²² Protección de datos personales (8 de marzo de 2014) Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3A114012>

En tercer lugar, El derecho a oponerse al tratamiento de los datos: el interesado deberá tener el derecho a oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento. También deberá tener la posibilidad de oponerse, previa petición y sin gastos, al tratamiento de los datos respecto de los cuales se prevea un tratamiento destinado a la prospección. Por último, deberá ser informado antes de que los datos se comuniquen a terceros a efectos de prospección y tendrá derecho a oponerse a dicha comunicación.²³

Así mismo esta directiva tiene tres aspectos relevantes que hay que remarcar:

Excepciones y limitaciones a los derechos del interesado: se podrá limitar el alcance de los principios relativos a la calidad de los datos, la información del interesado, el derecho de acceso y la publicidad de los tratamientos con objeto de salvaguardar, entre otras cosas, la seguridad del Estado, la defensa, la seguridad pública, la represión de infracciones penales, un interés económico y financiero importante de un Estado miembro o de la UE o la protección del interesado. **La confidencialidad y la seguridad del tratamiento:** las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento. Por otra parte, el responsable del tratamiento deberá aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados. **La notificación del tratamiento a la autoridad de control:** el responsable del tratamiento efectuará una notificación a la autoridad de control nacional con anterioridad a la realización de un tratamiento. La autoridad de control realizará comprobaciones previas sobre los posibles riesgos para los derechos y libertades de los interesados una vez que haya recibido la notificación. Deberá procederse a la publicidad de los tratamientos y las autoridades de control llevarán un registro de los tratamientos notificados.²⁴

²³ Protección de datos personales (8 de marzo de 2014) Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3A114012>

²⁴ Protección de datos personales (8 de marzo de 2014) Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3A114012>

2.2 NORMAS ACTUALES EN MATERIA DE PROTECCIÓN DE DATOS

2.2.1 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de Abril de 2016 (Reglamento general de protección de datos)

Este reglamento del que vamos a tratar de dar una explicación, es el instrumento principal para la protección de datos personales en el ámbito europeo y creador de todas las legislaciones nacionales sobre la protección de estos datos.

Esto nuevo reglamento aparece debido a la rápida evolución de la tecnología ya que esta causa que nazcan nuevos retos en cuanto a la protección de los datos que se encuentran en la red. Las personas cada vez comparten más datos personales y las empresas disponen de más capacidad para recoger y gestionar esos datos.²⁵

Todos estos cambios en el modelo de sociedad y en los medios tecnológicos requieren una regulación adecuada para la protección de datos en los países pertenecientes a la UE.

Según la propia web del Parlamento Europeo (PE) el objetivo del nuevo reglamento general es dar más control a los ciudadanos sobre su información privada en un mundo de teléfonos inteligentes, redes sociales, banca por internet y transferencias globales.

“Con este reglamento de protección de datos conseguimos un nivel uniforme de protección en toda la UE. Es un gran éxito para el Parlamento y un “sí” claro a los derechos de los consumidores y a la competencia en la era digital. Los ciudadanos podrán decidir por sí mismos qué información quieren compartir”, subrayó Jan Albrecht (Verdes, Alemania), responsable de la tramitación parlamentaria del texto.

“También se ofrece más claridad a las empresas, con una norma única para toda la UE que refuerza la confianza y la seguridad jurídica e impulsa la competencia justa”²⁶

²⁵ Resumen del Reglamento EU sobre la protección de datos de carácter personal. Recuperado en: <https://auditoria-lopd.es/resumen-del-reglamento-eu-la-proteccion-datos-caracter-personal/>

²⁶ Resumen del Reglamento EU sobre la protección de datos de carácter personal. Recuperado en: <https://auditoria-lopd.es/resumen-del-reglamento-eu-la-proteccion-datos-caracter-personal/>

Basandonos en esto este reglamento ofrece una gran claridad en cuanto al tratamiento de datos personales. Y no solo eso sino que el propio reglamento observa que el tratamiento de datos deben respetar los derechos y libertades fundamentales, cualquiera que sea la nacionalidad o residencia del ciudadano.

En sí el reglamento está concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.²⁷

Este reglamento introduce nuevas reglas como el conocido derecho al olvido, la necesidad de consentimiento claro y afirmativo, la portabilidad, el derecho a ser contactado si tus datos personales han sido pirateados, un lenguaje claro y adaptado para un humano medio sobre cláusulas de privacidad y multas de hasta 4% de la facturación global de las empresas en caso de infracción y derecho a indemnización.

3. NORMAS NACIONALES EN MATERIA DE PROTECCIÓN DE DATOS

La norma por excelencia y la cual vamos hablar en este apartado es la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

²⁷ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32016R0679>

Esta ley nace debido a las modificaciones sustanciales que lleva a cabo el Reglamento General de Protección de Datos.

El objeto principal de esta ley es la protección de las personas física en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismos.

Cabe decir que es una ley que se adapta a los nuevos tiempos. Con esto nos referimos al internet que se ha convertido en una realidad en la que se contiene nuestra vida personal tanto individual como colectiva. Casi toda nuestra actividad profesional, económica y privada se desarrolla en la propia red y adquiere una importancia fundamental.

Hoy identificamos con bastante claridad los riesgos y oportunidades que el mundo de las redes ofrece a la ciudadanía. Corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital. La transformación digital de nuestra sociedad es ya una realidad en nuestro desarrollo presente y futuro tanto a nivel social como económico. En este contexto, países de nuestro entorno ya han aprobado normativa que refuerza los derechos digitales de la ciudadanía.²⁸

Tras esta breve explicación por la cual se aprobó esta ley, vamos a explicar los aspectos más importantes que se destacan en esta ley:

1. La Ley obliga a las organizaciones cuyas actividades principales consistan en tratamientos que requieran una observación habitual y sistemática de los ciudadanos a gran escala a designar un **Delegado de Protección de Datos que cuente con la debida cualificación**.
2. Además de la designación, las organizaciones deberán garantizarle los medios necesarios para el ejercicio de sus funciones y notificar la designación a la AEPD para su inclusión en el **Registro público de Delegados de Protección de**

²⁸ Preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Datos.** Esto puede ocurrir ante el tratamiento a gran escala de categorías especiales de datos personales o datos relativos a condenas e infracciones penales.
3. El RGPD y la Ley Orgánica recogen varias bases jurídicas legitimadoras del tratamiento de datos personales por parte de las organizaciones privadas. Algunas de ellas son la relación contractual previa que contemple el tratamiento, el consentimiento del ciudadano o que el interés legítimo prevalezca sobre los derechos de las personas, por ejemplo. Por tanto, en la actualidad, no **resulta necesario que el particular consienta al tratamiento de sus datos personales si existe otra base jurídica que legitime el tratamiento.**
 4. La Ley Orgánica **garantiza el derecho a la intimidad de los empleados en el lugar de trabajo** frente al uso de dispositivos de videovigilancia y de grabación de sonidos, así como frente al uso de los dispositivos digitales y sistemas de geolocalización, de los que deberán ser informados de forma expresa, clara e inequívoca.
 5. Los contratos de encargo de tratamiento de datos personales entre las organizaciones (como responsables) y terceros (como encargados de tratamiento) suscritos antes del 25 de mayo de 2018 mantendrán su vigencia como máximo hasta el 25 de mayo de 2022 ²⁹

Estos son los cinco aspectos más importantes o que se pueden destacar de esta ley. Como podemos ver la propia ley crea diferentes organismos (Delegado de Protección de Datos, Registro público de Delegados de Protección de Datos) para controlar así el movimiento y el traspaso de los datos.

Además como nos referimos antes los propios trabajadores también están protegidos en su propio oficio al reservarles su derecho de intimidad frente al uso de dispositivos de videovigilancia. La propia ley remarca que se deberá informar de forma expresa, clara e inequívoca que se están utilizando estos recursos.

²⁹ Susana Romero (05-12-2019) *Análisis sobre la Ley Orgánica de Protección de datos y Garantía de los Derechos Digitales tras su primer año de aplicación* Recuperado en: <https://www.coordinacionempresarial.com/analisis-sobre-la-ley-organica-de-proteccion-de-datos-y-garantia-de-los-derechos-digitales-tras-su-primer-ano-de-aplicacion/>

Para finalizar esta ley pone en jaque a las empresas que tienen mucho más cuidado al tratar con los datos personales. Se estima según la Agencia Española de Protección de Datos que el número de reclamaciones en 2018 registró un aumento del 32,8% de las reclamaciones de particulares

4. ÓRGANOS EUROPEOS EN MATERIA DE PROTECCIÓN DE DATOS

En este apartado vamos a tratar de explicar cuales son los dos principales órganos europeos en materia de protección de datos.

La Unión Europea fue partidaria de crear dos órganos que fueran los controladores de la protección de datos personales. Con la entrada en el mundo del internet y de las redes sociales la propia Unión como hemos dicho se vio forzada a crear órganos que fueran los responsables de proteger los datos personales de los propios ciudadanos europeos.

Los dos órganos principales de protección de datos son:

1. Supervisor Europeo de Protección de Datos.
2. Comité Europeo de Protección de Datos

Hay que tener en cuenta que estos dos órganos no tienen una competencia en los datos personales tratados en el ámbito nacional. Pero si sobre todos los datos que estén moviéndose entre distintos ámbitos de la UE.

4.1 SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Se entiende que este supervisor de datos se trata de una autoridad independiente. Desde enero de 2004 el Supervisor Europeo de Protección de datos es D. Peter Hustinx. También cabe hacer mención a un Supervisor Adjunto que en este caso es Giovanni Buttarelli. Quién ha tomado esta decisión y ha otorgado los cargos a estas dos personas ha sido tanto el Parlamento Europeo como el Consejo. Su cometido es garantizar que las instituciones y los organismos de la Comunidad respeten el derecho fundamental a la protección de datos³⁰

Hay que remarcar que el propio SEPD (Supervisor Europeo de Protección de Datos), no tiene competencia sobre cuestiones de ámbito nacional, solo tiene competencia respecto de los datos tratados por las instituciones y organismos de la Comunidad.

El objetivo general del SEPD es garantizar que las instituciones y los organismos de la Comunidad respeten el derecho a la intimidad cuando realizan operaciones de tratamiento de datos personales o elaboran nuevas políticas.³¹

Se podría decir que el SEPD tiene tres ámbitos principales de actuación: control, asesoramiento y cooperación.

En cuanto al control: Tiene que llevar a cabo una supervisión de los datos personales que se manejan dentro de las instituciones y los organismos de la Comunidad. En segundo lugar, atender a las reclamaciones presentadas por parte de ciudadanos europeos cuyos datos se manejan en las instituciones y organismos europeos, incluyendo a los miembros que trabajan en la administración de la EU

En cuanto al asesoramiento: Responder las preguntas realizadas por los organismos o instituciones comunitarias que incidan sobre la protección de datos personales. El SEPD elabora dictámenes. Un rígido seguimiento de las innovaciones tecnológicas que afecten

³⁰ European Data Protection Supervisor. (2009). *El Supervisor Europeo de Protección de Datos y la protección de los datos personales en las instituciones y organismos comunitarios*. Recuperado en https://edps.europa.eu/sites/edp/files/publication/brochure_2009_es.pdf doi: 10.2804/2493

³¹ European Data Protection Supervisor. (2009). *El Supervisor Europeo de Protección de Datos y la protección de los datos personales en las instituciones y organismos comunitarios*. Recuperado en https://edps.europa.eu/sites/edp/files/publication/brochure_2009_es.pdf doi: 10.2804/2493

directamente a la protección de datos. Intervención en los procedimientos ante el Tribunal de Justicia³²

En cuanto a la cooperación: El SEPD puede cooperar con las autoridades nacionales para ofrecer una mayor protección. También coopera con grandes bases de datos como Eurodac.

Para finalizar se habla como antes hemos dicho de una función consultiva que desarrolla el SEPD a través de unos dictámenes. El SEPD en su primer mandato emitió casi 50 dictámenes. Entre las cuestiones tratadas en dichos dictámenes figuran la Decisión marco sobre protección de datos en el marco de la cooperación policial y judicial, la Directiva sobre la conservación de datos de telecomunicaciones, el Reglamento relativo al acceso del público a los documentos, el intercambio de datos con Estados Unidos, la Directiva sobre la intimidad y las comunicaciones electrónicas, y la comunicación sobre identificación por radiofrecuencia (RFID).³³

4.2 COMITÉ EUROPEO DE PROTECCIÓN DE DATOS

El CEPD es un órgano independiente que garantiza que la legislación de la UE en este ámbito, en concreto el Reglamento General de Protección de Datos (RGPD) y la Directiva sobre protección de datos en el ámbito penal, se aplique de forma coherente en todos los países que están regulados por ella, y promueve la cooperación entre las autoridades nacionales de protección de datos³⁴

³² European Data Protection Supervisor. (2009). *El Supervisor Europeo de Protección de Datos y la protección de los datos personales en las instituciones y organismos comunitarios*. Recuperado en https://edps.europa.eu/sites/edp/files/publication/brochure_2009_es.pdf doi: 10.2804/2493

³³ European Data Protection Supervisor. (2009). *El Supervisor Europeo de Protección de Datos y la protección de los datos personales en las instituciones y organismos comunitarios*. Recuperado en https://edps.europa.eu/sites/edp/files/publication/brochure_2009_es.pdf doi: 10.2804/2493

³⁴ Comité Europeo de Protección de Datos. Recuperado en: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-board_es#¿qué-hace-el-cepd?

El comité tiene una presidenta que en este caso es Andrea Jelinek y dos vicepresidentes que en este caso son Ventsislav Karadjov y Aleid Wolfsen. También está formado por las autoridades nacionales de protección de datos y el SEPD.

El propio CEPD (Comité Europeo de Protección de Datos) tiene 4 funciones principales:

1. Realiza distintas orientaciones generales para interpretar el propio Reglamento General de Protección de Datos
2. Adopta conclusiones para que el RGPD se interprete de una manera clara y coherente por parte de los organismos nacionales.
3. Su función más importante es la de asesorar a la Comisión Europea sobre las cuestiones que tienen relación sobre la protección de datos y sobre cualquier propuesta de la Legislación de la UE de especial importancia para la protección de datos personales³⁵
4. Anima a las autoridades nacionales de protección de datos a colaborar y compartir información y buenas prácticas entre sí.

El CEPD garantiza que las normas sobre protección de datos personales se apliquen de forma adecuada para ello:

- Publica directrices para que las autoridades nacionales y las partes interesadas garanticen una interpretación coherente del RGPD.
- Adopta conclusiones sobre coherencia para que las autoridades reguladoras nacionales garanticen que los derechos y obligaciones jurídicas correspondientes se apliquen del mismo modo en todos los países.
- También es una fuente de conocimientos especializados sobre cuestiones de protección de datos, que asesora a la Comisión Europea. Esto garantiza que cualquier nueva legislación de la UE que presente un impacto de especial

³⁵ Comité Europeo de Protección de Datos. Recuperado en: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-board_es#¿qué-hace-el-cepd?

importancia en este ámbito respete el derecho fundamental a la protección de los datos de carácter personal.³⁶

5. ÓRGANOS ESTATALES DE PROTECCIÓN DE DATOS

Los principales órganos estatales en materia de protección de datos son el delegado protección de datos y la agencia española de protección de datos. Ambos órganos velan porque los datos transmitidos entre administraciones de ciudadanos españoles sean utilizados de una forma correcta.

En los siguientes epígrafes se va a comenzar a explicar los dos órganos anteriormente mencionados destacando sus funciones principales y los aspectos más importantes de estos.

5.1 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Este es el principal organismo en relación con la protección de datos. Se trata de un ente público que tiene una propia personalidad jurídica y que actúa con independencia y suele relacionarse con el Ministerio de Justicia.

Su régimen jurídico se regula en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que prevé además que el Gobierno, a propuesta de la propia AEPD, aprobará su estatuto mediante Real Decreto. También le es de aplicación la Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público.³⁷

³⁶ Comité Europeo de Protección de Datos. Recuperado en: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-board_es#¿qué-hace-el-cepd?

³⁷ Guías Jurídicas Wolterskluwer. (Febrero 2020). “Especial Protección de Datos. La privacidad al Servicio de la Ciudadanía”. Recuperado en: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAEAMtMSbF1jTAAAUNDU0NLtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoArv0c4zUAAAA=WKE

Las funciones más importantes o destacables de la AEPD (Agencia Española de Protección de Datos)

En primer lugar, la AEPD emite autorizaciones, circulares, directrices y atienden peticiones y reclamaciones formuladas por personas afectadas. También proporciona la información necesaria a las personas para que estas conozcan los derechos en materia de tratamiento de sus datos personales. Este organismo puede llegar a cesar o suspender los transferencias internacionales de datos si no se cumple con la normativa europea o la española.

En segundo lugar, le corresponde asimismo redactar su Memoria anual, que remite al Ministerio de Justicia, y elabora y aprueba su anteproyecto de presupuesto.³⁸

En tercer lugar, hay un cooperación con organismos internacionales y también con distintas instituciones de la UE. En particular, presta asistencia a las autoridades designadas por los Estados parte en el Convenio 108 del Consejo de Europa de 28 de enero de 1981, sobre protección de las personas en relación con el tratamiento automatizado de los datos de carácter personal, a los efectos previstos en el artículo 13 del Convenio, siendo necesario tener en consideración que este Convenio fue actualizado en 2018, y respecto del Sistema de Información Schengen ejerce el control de los datos de carácter personal introducidos en la parte nacional española de la base de datos del citado Sistema.³⁹

Se habla también de unas competencias sancionadoras previstas en las siguientes leyes: Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones y de la Ley 59/2003, de 19 de diciembre.

³⁸ Guías Jurídicas Wolterkluwer. (Febrero 2020). “Especial Protección de Datos. La privacidad al Servicio de la Ciudadanía”. Recuperado en: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAEAMtMSbF1jTAAAUNDU0NLtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoArv0c4zUAAAA=WKE

³⁹ Guías Jurídicas Wolterkluwer. (Febrero 2020). “Especial Protección de Datos. La privacidad al Servicio de la Ciudadanía”. Recuperado en: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAEAMtMSbF1jTAAAUNDU0NLtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoArv0c4zUAAAA=WKE

En cuanto como es su organización interna. Pues la AEPD esta conformada por una presidencia, un consejo consultivo, el registro general de protección de datos, la inspección de datos y la secretaría general de la agencia.

- En cuanto a la Presidencia, es la que representa a la propia agencia. Sus funciones son la de dirección y gestión. La competencia de la presidencia es dictar resoluciones sobre tutelas de derechos, transferencias internacionales, procedimientos sancionadores.
- En cuanto al Consejo Consultivo, es un órgano colegiado, con quince vocales nombrados por el Ministerio de Justicia. Informa de todas las cuestiones que se le soliciten⁴⁰
- En cuanto al Registro General de protección de datos, su función principal es la de gestionar el registro de delegados de protección así como la de crear códigos de conducta.
- En cuanto a la inspección de datos, ejerce funciones inspectoras e instructoras. Instruye los expedientes que resuelve la presidencia.⁴¹
- En cuanto a la Secretaria General de la Agencia: Desempeña tareas de apoyo, también elabora informes y propuestas que le solicite la propia Presidencia.⁴²

Por último remarcar que la propia Agencia esta controlada por el Tribunal de Cuentas y por la propia Administración del Estado.

⁴⁰ Guías Jurídicas Wolterkluwer. (Febrero 2020). “Especial Protección de Datos. La privacidad al Servicio de la Ciudadanía”. Recuperado en:

https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUNDU0NLtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoArv0c4zUAAAA=WKE

⁴¹ Guías Jurídicas Wolterkluwer. (Febrero 2020). “Especial Protección de Datos. La privacidad al Servicio de la Ciudadanía”. Recuperado en:

https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUNDU0NLtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoArv0c4zUAAAA=WKE

⁴² Guías Jurídicas Wolterkluwer. (Febrero 2020). “Especial Protección de Datos. La privacidad al Servicio de la Ciudadanía”. Recuperado en:

https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUNDU0NLtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoArv0c4zUAAAA=WKE

5.2 DELEGADO DE PROTECCIÓN DE DATOS

El delegado de protección de datos es otro instrumento esencial en el tratamiento de datos de los ciudadanos españoles. Es el propio RGPD el que introduce esta figura, la cual debe ser designada por los entes de la Administración Local.

La norma europea señala que el Delegado de Protección de Datos será una persona con conocimiento especializado en Derecho y en la práctica en materia de protección de datos. Estos conocimientos serán exigibles en relación con los tratamientos que se realicen, así como las medidas que deban adoptarse para garantizar un tratamiento adecuado de los datos personales objeto de esos tratamientos.⁴³

El delegado tiene una serie de funciones que se encuentran en el artículo 39 RGPD:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones del RGPD y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al artículo 35 del RGPD.
- Cooperar con la Autoridad de control.

⁴³ Guías sectoriales AEPD. “*Protección de datos y administración local*”. Recuperado en: <https://www.aepd.es/sites/default/files/2019-09/guia-proteccion-datos-administracion-local.pdf>

- Actuar como punto de contacto de la Autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.⁴⁴

Por último remarcar, que el trabajo que desarrolle el DPD (Delegado de Protección de Datos) dependerá de la entidad que se adscriba. Esto quiere decir no es lo mismo desarrollar un trabajo en una entidad de gran tamaño que en una pequeña.

6. ÓRGANOS ESPECIALES EN CATALUÑA Y PAÍS VASCO

Como hemos dicho anteriormente cada Comunidad Autónoma debe desarrollar su labor en cuanto a la protección de datos. Antes hemos recordado que el Delegado de Protección de Datos tendrá mas carga laboral o menos dependiendo a la entidad a la que se adscriba. Eso debe a que hay entidad de gran tamaño y otras más pequeñas.

Las dos que vamos a distinguir aquí son la Autoridad Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos.

6.1 AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS

La Autoridad Catalana de Protección de Datos (APDCAT) es un organismo independiente que vela para garantizar, en el ámbito de las competencias de la Generalitat, los derechos a la protección de datos personales y de acceso a la información que está vinculada. Desde este organismo, se informa sobre cuáles son los derechos en esta materia, cómo se ejercen y qué se debe hacer si no se respetan. La APDCAT también informa y asesora sobre las obligaciones que prevé la legislación y controla que las entidades las cumplan.⁴⁵

Como se puede tener en mente el ámbito de competencia de este organismo público esta dentro de la Comunidad Autónoma de Cataluña.

⁴⁴ Artículo 39 del Reglamento General de Protección de Datos. Recuperado en: <https://www.privacy-regulation.eu/es/39.htm>

⁴⁵ Autoridad Catalana de Protección de Datos. 2018. Recuperado en: https://apdcatal.gencat.cat/es/autoritat/estructura/autoritat_catalana_de_proteccio_de_dades/

Basicamente lo que lleva a cabo la APDCAT es el control de los datos de las instituciones públicas, de la Administración de la Generalitat, los entes locales, las entidades autónomas y las entidades de derecho privado que forman parte de la Generalitat.

Además la ley la Ley 32/2010, del 1 de octubre, de la Autoridad Catalana de Protección de Datos, entre otras funciones regula las de:

- Responder las consultas que formulan las entidades de su ámbito de actuación sobre la protección de datos de carácter personal en poder de las administraciones públicas y colaborar con estas entidades, en la difusión de las obligaciones derivadas de la legislación reguladora de estas materias.
- Emitir el informe preceptivo sobre las disposiciones que afectan a la protección de datos de carácter personal.
- Elaborar planes de auditoría.⁴⁶

Finalmente cabe decir que la APDCAT esta formada por un Órgano de Gobierno, un Director, un Consejo Asesor de Protección de Datos y el Registro de Protección de Datos de Cataluña.

6.2 AGENCIA VASCA DE PROTECCIÓN DE DATOS.

Se trata de un órgano de derecho público, con personalidad jurídica y que actúa con plena independencia.

Sus funciones se encuentran en el artículo 17 de la Ley 2/2004. Esta artículo enumera hasta 15 funciones. En resumidas cuentas, lo que hace Agencia Vasca de Protección datos es velar por el cumplimiento de la legislación sobre protección de datos

⁴⁶ Autoridad Catalana de Protección de Datos. 2018. Recuperado en: https://apdcat.gencat.cat/es/autoritat/estructura/autoritat_catalana_de_proteccio_de_dades/

y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos ⁴⁷

Su estructura esta formada por un Director al que le asesora un Consejo Consultivo. Por debajo de este se encuentra una Asesoría Jurídica e Inspección esta da instrucción a los procedimientos tanto de infracción como de reclamación de los ciudadanos. Paralela a esta se encuentra un Registro y Auditoría de ficheros de datos de carácter personal que es donde se recogen los datos personales que se encuentren dentro del ámbito de aplicación de la ley. Por último, nos encontramos al mismo nivel la Secretaría General que tiene la función de gestionar los recursos humanos y materiales.

7. ASPECTOS A DESTACAR DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

Anteriormente en el epígrafe 2.2 hemos hablado y desarrollado en general el Reglamento General de Protección de Datos. En este epígrafe lo que se va a ver son los aspectos más destacables de este Reglamento y que difieren de la antigua legislación.

Estos aspectos o puntos importantes los vamos a ir desarrollando uno por uno y son los siguientes:

- I. Sanciones a empresas
- II. Consentimiento y transparencia
- III. Registro de actividades de tratamiento
- IV. Análisis de riesgos y evaluaciones de impactos
- V. Ejercicio de derechos
- VI. Terceros
- VII. Big data

⁴⁷ Agencia Vasca de Protección de Datos. Recuperado en: <https://www.avpd.euskadi.eus/informacion/informacion-institucional-y-organizacional-composicion-y-personal/s04-5216/es/>

7.1 SANCIONES A EMPRESAS

Este es un gran cambio que ha llegado de sorpresa a las grandes empresas. Está claro que ya eran muy fuertes las sanciones establecidas por la LOPD que podían llegar hasta un máximo de 600.000 euros. El Reglamento aumenta esta cantidad fijando límites de hasta 10 millones de euros y 20 millones de euros para las infracciones graves y muy graves.

Por otra parte, el Reglamento no establece cuáles son las sanciones leves, sino que atribuye a los Estados la competencia para establecerlas. Competencia que, por cierto, el Estado español no ha ejercido en el proyecto de LOPD que se tramita en el Congreso y, salvo que se enmiende este problema en su tramitación parlamentaria, el sistema jurídico español adolecerá de tipificación de las sanciones aplicables a las infracciones distintas de las que el RGPD sanciona con multas económicas, lo que puede ser un problema muy grave en la práctica.⁴⁸

7.2 CONSENTIMIENTO Y TRANSPARENCIA

Según el RGPD el consentimiento no se considera la clave de la legitimación para el tratamiento de datos, dejándolo para algunos supuestos como la excepción o derogación de la necesidad de consentimiento.

En el caso de consentimiento se necesita que se cumplan los siguientes requisitos: libre, específico, informado e inequívoco. Por lo tanto se entiende que ya no tiene potestad el consentimiento tácito y tampoco el consentimiento cuando no se tenga la oportunidad de oponerse, porque entonces no es libre.

Por último la transparencia obliga a organizar el sistema de tratamiento de datos de forma que el interesado conozca siempre todas sus circunstancias, que no haya ningún aspecto que le sorprenda en ningún momento.⁴⁹

⁴⁸ Revista del Consejo General de Abogacía. Nº 109. Mayo de 2018.

⁴⁹ Revista del Consejo General de Abogacía. Nº 109. Mayo de 2018.

7.3 REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Todas las empresas o compañías que tengan más de 250 trabajadores o que traten con datos sensibles generaran riesgos. Por lo tanto, los interesados tienen que mantener actualizado un registro donde se puedan ver los distintos tratamientos de datos. En este caso, esta función recae sobre los encargados de tratamiento .

Para elaborar este registro es preciso recopilar toda la información relativa al procesamiento y utilización de la información, lo que involucra necesariamente a todas las áreas de la compañía. El RGPD dará lugar a la desaparición en España del Registro de ficheros de la AEPD⁵⁰

7.4 ANÁLISIS DE RIESGOS Y EVALUACIONES DE IMPACTOS

Cuando ya se ha iniciado y identificado las actividades de tratamiento de datos personales, entonces la propia empresa deberá analizar que riesgos afectan a cada una de ellas. Este análisis se debe hacer desde una perspectiva que beneficie al individuo y no desde el punto de vista de la compañía como era antes de que entrará en vigor el RGPD.

El propio Reglamento obliga a realizar lo que se conoce como Evaluaciones de Impactos en Privacidad (Privacy Impact Assesments) si uno de estos tratamientos genera un alto riesgo y afecta a los derechos o libertades de las personas físicas debido a su naturaleza o alcance.

La EIPD es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar

⁵⁰ Revista del Consejo General de Abogacía. Nº 109. Mayo de 2018.

el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.⁵¹

7.5 EJERCICIO DE DERECHOS

En este ámbito lo más importante es destacar el derecho a la portabilidad. Esta obliga al responsable a facilitar una copia completa de los datos personales tanto en soporte electrónico como en un soporte compatible.

Se incluyen todo los datos que se obtengan del uso o desarrollo del servicio contratado como historial de búsquedas, tráfico, localización, etc. Lo que se llega a excluir son los datos derivados o sacados por la empresa mediante el mecanismo del know how.

Por otra parte, el derecho de acceso se amplía con el RGPD, obligando al responsable a facilitar una copia de los datos personales objeto de tratamiento (en formato no digital, lógicamente, pero sin limitación respecto de los datos inferidos). Este cambio tendrá un impacto muy importante en los costes de su atención, aunque la norma permite cobrar un canon razonable por la obtención de copias adicionales.⁵²

7.6 TERCEROS

El RGPD amplía enormemente las responsabilidades de los prestadores de servicios. Además, se responsabiliza a la compañía de la selección y control de sus encargados. Esto obliga a las compañías a establecer procesos de homologación de proveedores, para poder acreditar que tienen un protocolo adecuado de selección de encargados idóneos y a llevar a cabo controles y seguimientos.⁵³

⁵¹ Agencia Española de Protección de Datos. “*Guía práctica para LAS Evaluaciones de Impacto en la Protección de LOS datos sujetas al RGPD*”. Recuperado en: <https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf>

⁵² Revista del Consejo General de Abogacía. N° 109. Mayo de 2018.

⁵³ Revista del Consejo General de Abogacía. N° 109. Mayo de 2018.

7.7 BIG DATA

Otro cambio es que la RGPD da importancia a la generación de los perfiles de las personas.

Los incluye dentro de su ámbito tanto a una necesidad de consentimiento como al sometimiento a los principios de protección. Las auditorías periódicas de los algoritmos para evitar situaciones discriminatorias, la pseudonimización y anonimización, la intervención humana en partes del proceso, la transparencia y audiencia al usuario serán elementos de garantía a la hora de llevar a cabo estas prácticas.⁵⁴

Sin duda se tienen que cambiar muchas cosas en las empresas para que estas se adapten a la disposición del 25 de mayo de 2018.

8. CONCLUSIONES Y VISTAS DE FUTURO DE LA PROTECCIÓN DE DATOS

En este epígrafe voy a dar mi opinión sobre como creo que se va a desarrollar la protección de datos en un futuro y lo que creo que se puede mejorar. Así como unas conclusiones.

Desde mi punto de vista, la protección de los datos personales esta siendo un ámbito muy importante en estos días. En la actualidad, miles de datos se comparten por internet y por las redes sociales. La pregunta es donde se encuentra el límite para compilar nuestros datos personales por parte de la empresas. Siempre se habla de que empresas como Facebook, Instagram o Google nos “espían” o conocen datos nuestros sin nuestro consentimiento.

⁵⁴ Revista del Consejo General de Abogacía. Nº 109. Mayo de 2018.

Por ello, no solo nuestro país sino además la UE ha estado regulando rápidamente para abarcar en este campo de las redes sociales. El gran problema que he visto yo es que la tecnología avanza a una velocidad desorbitada y el derecho no es capaz ir a la velocidad de esta.

Esta claro que el RGPD da una visión bastante clara y genera una protección importante, sobretodo estableciendo unas sanciones muy gravosas, en sentido económico, para las empresas. Aún así recordemos, 10 millones para una empresa como Facebook o Google no es tanto.

Sigue ocurriendo que por ejemplo Facebook nos enseña anuncios sobre cosas que hemos hablado o conversado con otra persona. Las personas se preguntan de donde han conseguido esos datos. La mayoría de la gente no conoce que es la protección de datos y como funciona, por lo tanto ve normal que Facebook u otras plataformas hagan esto.

De lo que si habla el RGPD es del gran derecho al olvido. Que básicamente es el derecho a impedir la difusión de su información personal a través de internet. Muchas veces este derecho no se suele cumplir por parte de las empresas.

En conclusión, creo que si hay una buena regulación de protección de datos protegiendo así al ciudadano. Los dos grandes problemas que habría que resolver es que las propias empresas muchas veces incumplen la regulación de protección de datos. Y el otro problema es que la forma de transmitir datos cada vez se hace de forma distinta exigiendo que la legislación sea más exacta y más dura para proteger este tratamiento de datos personales. Se podrían dar distintas soluciones para resolver los distintos problemas que hemos ido enumerando.

1. Creo que debería de haber un régimen que fuera más duro con la protección de datos es decir que pudiera controlar mucho más el movimiento de datos sobre todo de las empresas que son los principales organismos que reciben y envían datos. Todas estas empresas como hemos visto están sujetas a una serie de controles y sanciones en el RGPD. Pero desde mi más sincera opinión, creo que las sanciones son mínimas si se tratan de una empresa internacional como puede ser Google o Apple. Por lo tanto insto no solo a nuestro país sino a la Unión Europea y a la Comunidad Internacional a que

desarrollen un sistema de control mucho más restrictivo y que las sanciones sean mas duras.

2. En mi opinión, creo que otro punto importante y que se ha nombrado anteriormente es el derecho al olvido. Desde mi punto de vista, este derecho al olvido daría la solución a muchos problemas. Todos los datos contenidos en internet que queremos borrar no desaparecen del todo, pero con el nombrado derecho al olvido esta información tendría que desaparecer por ley. Pienso que el derecho al olvido debe ser implementado para que todos esos datos que no tienen cabida y quieren ser borrados desaparezcan de la red.

3. Por lo tanto y para concluir definitivamente, como hemos dicho anteriormente creo que la Unión Europea tendría que estar constantemente legislado sobre la protección de datos debido a que es una materia que esta en constante desarrollo ya que toca de muy cerca la tecnología. Esto hace que la transmisión de información cambie de un año para otro y por ello la legislación debe avanzar con estos cambios

9. BIBLIOGRAFÍA

- Constitución Española de 1978
- Sentencia del Tribunal Constitucional 94/1998 de 4 de Mayo.
- Sentencia del Tribunal Constitucional 292/2000 de 30 de Noviembre.
- Conde Ortiz, Concepción . 2005. “*La protección de datos personales un derecho autónomo con base en los conceptos de intimidad y privacidad*”. Dykinson
- Sardina Ventosa, F., op. cit., p.1
- Uría Menéndez. Diciembre 2018. *Principales novedades de la nueva Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales*. pág. 2.
- DAVARA RODRÍGUEZ, M. A.: *La protección de datos personales en el sector de las telecomunicaciones*, cit., p. 9.
- URABAYEN, M., op. cit., p. 9
- La protección de datos personales (Enero de 2020). Recuperado de <https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales>.
- Cfr. S. Ripoll Carulla, “En torno a la calificación de la pasividad española en el cumplimiento del Convenio n.o 108 del Consejo de Europa como

acto ilícito internacional”, en *La responsabilidad internacional*, XII Jornadas de la A.E.P.D.I.R.I., Alicante, 1990, págs. 313 – 330

- Convenio 108 del Consejo de Europa
- D. Juan Antonio Pavón Perez (Profesor de Derecho Internacional Público). Universidad de Extremadura. *La protección de datos personales en el consejo de europa: El protocolo adicional al Convenio 108 Relativo a las autoridades de control y a los flujos transfronterizos de datos personales.*
- Vid. J. Carrascosa González, «Protección de la intimidad y tratamiento automatizado de datos de carácter personal en Derecho internacional Privado», *Revista Española de Derecho Internacional*, vol. XLIV, 1992, págs. 417-441; G. Garzón y E. Vilariño, «Information and Privacy Protection in TDF: The Rights Involved», en O.C.D.E., *TDF and the Protection of Privacy*, págs. 306 y ss; D. H. Flaherty, *Privacy and Government Data Banks: an International Perspective*, Londres, Mansell, 1979; R. N. Savage y I. N. Waldenn, «Data Protection and Privacy Laws: Should Organisations Be Protected», *I.C.L.Q.*, 1988, págs. 37 y ss.
- Protección de datos personales (8 de marzo de 2014) Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3A114012>
- Resumen del Reglamento EU sobre la protección de datos de carácter personal. Recuperado en: <https://auditoria-lopd.es/resumen-del-reglamento-eu-la-proteccion-datos-caracter-personal/>
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de

protección de datos) Recuperado en: <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32016R067>

- Preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Susana Romero (05-12-2019) *Análisis sobre la Ley Orgánica de Protección de datos y Garantía de los Derechos Digitales tras su primer año de aplicación* Recuperado en: <https://www.coordinacionempresarial.com/analisis-sobre-la-ley-organica-de-proteccion-de-datos-y-garantia-de-los-derechos-digitales-tras-su-primer-ano-de-aplicacion/>
- European Data Protection Supervisor. (2009). *El Supervisor Europeo de Protección de Datos y la protección de los datos personales en las instituciones y organismos comunitarios*. Recuperado en https://edps.europa.eu/sites/edp/files/publication/brochure_2009_es.pdf doi: 10.2804/2493
- Comité Europeo de Protección de Datos. Recuperado en: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-board_es#¿qué-hace-el-cepd?
- Guías Jurídicas Wolterkluwer. (Febrero 2020). *“Especial Protección de Datos. La privacidad al Servicio de la Ciudadanía”*. Recuperado en: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbFljTAAAUNDU0NLtbLUouLM_DxbIwMD_CwNzAwuQQGZapUt-ckhlQaptWmJOcSoArv0c4zUAAAA=WKE
- Guías sectoriales AEPD. *“Protección de datos y administración local”*. Recuperado en: <https://www.aepd.es/sites/default/files/2019-09/guia-proteccion-datos-administracion-local.pdf>
- Reglamento General de Protección de Datos

- Autoridad Catalana de Protección de Datos. 2018. Recuperado en: https://apdcat.gencat.cat/es/autoritat/estructura/autoritat_catalana_de_proteccio_de_dades/
- Agencia Vasca de Protección de Datos. Recuperado en: <https://www.avpd.euskadi.eus/informacion/informacion-institucional-y-organizacional-composicion-y-personal/s04-5216/es/>
- Revista del Consejo General de Abogacía. Nº 109. Mayo de 2018.
- Agencia Española de Protección de Datos. “*Guía práctica para LAS Evaluaciones de Impacto en la Protección de LOS datos sujetas al RGPD*”. Recuperado en: <https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf>